

On Some Properties of Quadratic APN Functions of a Special Form

Irene Villa
Department of Informatics
University of Bergen
Bergen, Norway
Irene.Villa@uib.no

Abstract—In a recent paper [1], it is shown that functions of the form $L_1(x^3) + L_2(x^9)$, where L_1 and L_2 are linear, are a good source for construction of new infinite families of APN functions. In the present work we study necessary and sufficient conditions for such functions to be APN.

I. INTRODUCTION

For given positive integers n and m , a function F from the finite field with 2^n elements to the finite field with 2^m elements is called a vectorial Boolean function or an (n, m) -function, and in the case when $m=1$ it is simply called a Boolean function. Boolean functions are among the most fundamental objects investigated in pure and applied mathematics and computer science. Boolean function theory is an important tool for solving problems of analysis and synthesis of discrete devices which transform and process information. The primary motivation for studying Boolean functions comes from cryptography. In modern society, exchange and storage of information in an efficient, reliable and secure manner is of fundamental importance. Cryptographic primitives are used to protect information against eavesdropping, unauthorized changes and other misuse. In the case of symmetric cryptography ciphers are designed by appropriate composition of nonlinear Boolean functions. For example, the security of block ciphers depends on S-boxes which are (n, m) -functions. For most of cryptographic attacks on block ciphers there are certain properties of functions which measure the resistance of the S-box to these attacks. The differential attack introduced by Biham and Shamir is one of the most efficient cryptanalysis tools for block ciphers. It is based on the study of how differences in an input can affect the resulting difference at the output. When $n = m$ the functions that contribute an optimal resistance against differential attack are called *Almost Perfect Nonlinear* (APN). Such APN function $F(x)$ are characterized by having at most two solution for every equation $F(x + a) - F(x) = b$, where a and b are general elements of the field and a is not null.

The role of APN functions is not just related to cryptography. In coding theory APN functions define binary error correcting codes optimal in a certain sense. In projective geometry quadratic APN functions define dual hyperovals. Recent advances in APN functions have made a prominent impact on the theory of commutative semifields.

For these reasons many works were focused on the studying and the construction of such optimal functions.

Let assume n be a positive integer and \mathbb{F}_{2^n} the finite field with 2^n elements. If n is an even number, then we have that $3|(2^n - 1)$ and we denote with k the integer value $\frac{2^n - 1}{3}$. A function F from \mathbb{F}_{2^n} to \mathbb{F}_{2^n} admits a unique representation, called *Univariate Polynomial Representation*, over \mathbb{F}_{2^n} of degree at most $2^n - 1$:

$$F(x) = \sum_{j=0}^{2^n-1} \delta_j x^j, \text{ with } \delta_j \in \mathbb{F}_{2^n}.$$

For every integer j consider its binary expansion $\sum_{s=0}^{n-1} j_s 2^s$ and denote with $w_2(j)$ the number of nonzero coefficients (i.e. $\sum_{s=0}^{n-1} j_s$). The *algebraic degree* of the function F is the $\max_{j=0, \dots, 2^n-1, \delta_j \neq 0} w_2(j)$. Functions of algebraic degree 1 are called *affine* and of degree 2 *quadratic*. *Linear functions* are affine functions without the constant term and they can be represented as $L(x) = \sum_{j=0}^{n-1} \gamma_j x^{2^j}$. A known example of a linear function defined over any dimension n is the *Trace function* $Tr(x) = Tr_n(x) = \sum_{i=0}^{n-1} x^{2^i}$. In particular the trace is a Boolean function, i.e. $Tr : \mathbb{F}_{2^n} \rightarrow \mathbb{F}_2$. For m positive divisor of n we use the notation $Tr^m(x) = \sum_{i=0}^{n/m-1} x^{2^{im}}$.

Given a function F we define its λ -component as the Boolean function $f_\lambda : \mathbb{F}_{2^n} \rightarrow \mathbb{F}_2$ with $f_\lambda(x) = Tr(\lambda \cdot F(x))$, for $\lambda \in \mathbb{F}_{2^n}$. For a Boolean function f we define the Walsh transformation as

$$\hat{f}_\chi(u) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x) + Tr(ux)},$$

with $u \in \mathbb{F}_{2^n}$. With *Walsh Spectrum* we refer to the set of all possible values of the Walsh transformation. With the symbol $\mathcal{F}(f)$ we indicate the Walsh transformation valued in 0,

$$\mathcal{F}(f) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x)} = 2^n - 2 \cdot \text{wt}(f),$$

where $\text{wt}(f)$ is the Hamming weight of f (i.e. the cardinality of the set $\{x \in \mathbb{F}_{2^n} : f(x) = 1\}$). Therefore we have that a Boolean function f is balanced ($\text{wt}(f) = 2^{n-1}$) if and only if $\mathcal{F}(f) = 0$. A Boolean function f is called *bent* if its Walsh spectrum corresponds to the set $\{\pm 2^{n/2}\}$. Therefore such function can exist only for even values of n . Moreover,

we have that f is bent if and only if, for every $a \in \mathbb{F}_{2^n}^*$, the function $D_a f(x) = f(x+a) + f(x)$ is balanced.

For every nonzero element $a \in \mathbb{F}_{2^n}^*$ the *derivative* of F in the direction of a is the function $D_a F(x) = F(x+a) + F(x)$. The function F is called *almost perfect nonlinear* (APN) if for every $a \neq 0$ and every b in \mathbb{F}_{2^n} , the equation $D_a F(x) = b$ admits at most 2 solutions. Used as S-Boxes in block ciphers, APN functions are useful since they oppose an optimal resistance against differential cryptanalysis.

The APN property is invariant under the action of some transformations of functions.

- Given A_1, A_2 affine permutations and A an affine function, if F is APN then also $G = A_1 \circ F \circ A_2 + A$ is APN; in this case the functions are called *extended affine equivalent* (EA-equivalent).
- Two functions F and G are *CCZ-equivalent* if there exists an affine permutation \mathcal{L} of $\mathbb{F}_{2^n}^2$ such that $\mathcal{L}(\Gamma_F) = \Gamma_G$, where Γ_F is the graph of the function F , $\{(x, F(x)) : x \in \mathbb{F}_{2^n}\}$. Also CCZ-equivalence preserve the APN property. Moreover, we have that EA-equivalence is a particular case of CCZ-equivalence.

Many different works have been focused on finding and constructing new families of APN functions. Table I gives us all known values for exponents d such that the function x^d , defined over \mathbb{F}_{2^n} , is APN.

Since EA-equivalence preserves the algebraic degree of a function and, in general, the functions listed in Table I have different algebraic degrees, it is easy to verify that these APN functions are EA-inequivalent. Instead the algebraic degree is not an invariant for CCZ-equivalence. But also for this case it was possible to prove some inequalities. In [10] it is shown that two different Gold functions x^{2^i+1} and x^{2^j+1} , where $1 \leq i < j \leq n/2$, are CCZ-inequivalent and that in general the Gold functions are CCZ-inequivalent to the Welch and to any Kasami functions. Moreover, the inverse and Dobbertin functions are not CCZ-equivalent to each other and to all other known APN power functions, [10]. For all the other cases the problem is still open.

Before the work in [11] the only known APN functions were EA-equivalent to power functions and it was supposed that all APN functions are EA-equivalent to power functions. In [11] it is showed the existence of classes of APN mappings EA-inequivalent to power functions. Such functions

were constructed by applying CCZ-equivalence to the Gold APN mappings. In [12] we can find the first examples of APN function CCZ-inequivalent to power functions. The first infinite families of such APN polynomial can be found in [11]. In Table II these functions are listed. They are all quadratic functions.

In this work we focus on functions of the form

$$F'(x) = F(x^3) = L_1(x^3) + L_2(x^9), \quad (1)$$

where L_1 and L_2 are linear functions. From now on, we will refer to L_1 and L_2 as to the linear functions

$$L_1(x) = \sum_{i=0}^{n-1} b_i x^{2^i} \text{ and } L_2(x) = \sum_{i=0}^{n-1} c_i x^{2^i}, \quad (2)$$

with $b_i, c_i \in \mathbb{F}_{2^n}$. In particular we want to study conditions on L_1 and L_2 such that F' is APN.

Some results are already been given in different papers. In [15] the function $x^3 + \text{Tr}(x^9)$ is proved to be APN for any dimension n . Moreover, for $n \geq 7$ it is proved to be CCZ-inequivalent to the Gold functions, to the inverse and Dobbertin functions and EA-inequivalent to power functions. For a quadratic APN function $F : \mathbb{F}_{2^n} \rightarrow \mathbb{F}_{2^n}$ and a quadratic boolean function $f : \mathbb{F}_{2^n} \rightarrow \mathbb{F}_2$, under some conditions it is proved that the function $F(x) + f(x)$ is APN. In particular these conditions are that for every nonzero $a \in \mathbb{F}_{2^n}$ there must exist a linear Boolean function l_a satisfying:

- 1) $\varphi_f(x, a) = l_a(\varphi_F(x, a))$,
- 2) if $\varphi_F(x, a) = 1$ for some $x \in \mathbb{F}_{2^n}$ then $l_a(1) = 0$,

where $\varphi_\chi(x, a) = \chi(x) + \chi(x+a) + \chi(a) + \chi(0)$.

A similar theorem is proved when $f : \mathbb{F}_{2^n} \rightarrow \mathbb{F}_{2^m}$, where m is a divisor of n . Due to this result the following functions, defined over $\mathbb{F}_{2^{2m}}$ where m is an even positive integer, are APN:

- $x^3 + \text{Tr}_{n/m}(x^{2^m+2}) = x^3 + x^{2^m+2} + x^{2^{m+1}+1}$,
- $x^3 + (\text{Tr}_{n/m}(x^{2^m+2}))^3$.

When F is a Gold function, all possible APN mappings $F(x) + f(x)$, where f is a Boolean function, are computed until dimension 15. The only possibilities, different from $x^3 + \text{Tr}(x^9)$, are for $n = 5$ the function $x^5 + \text{Tr}(x^3)$ (CCZ-equivalent to Gold functions) and for $n = 8$ the function $x^9 + \text{Tr}(x^3)$ (CCZ-inequivalent to power functions and to $x^3 + \text{Tr}(x^9)$).

In [1] the function $x^3 + \text{Tr}(x^9)$ has been generalized to form (1). It has been proved that for n even a sufficient condition is $L_1(x) + L_2(x^3)$ being a permutation over \mathbb{F}_{2^n} . In the odd dimension a weaker conditions lead to an APN mapping.

Moreover from the fact that by applying a linear function $l(x) = ax + b$, with $a \in \mathbb{F}_{2^n}^*$ and $b \in \mathbb{F}_{2^n}$, to a permutation we obtain another one, a simply but useful statement has been proved. In particular it is stated that for n even, L a linear function over \mathbb{F}_{2^n} , $a \in \mathbb{F}_{2^n}^*$ and $b \in \mathbb{F}_{2^n}$ if $x + L(x^3)$ is a permutation over \mathbb{F}_{2^n} , then the function

$$ax^3 + L(a^3x^9 + a^2bx^6 + ab^2x^3) \quad (3)$$

Table I
KNOWN APN POWER FUNCTIONS x^d OVER \mathbb{F}_{2^n}

Functions	Exponents d	Conditions	Degree	Proven
Golden	$2^i + 1$	$\gcd(i, n)=1$	2	[2], [3]
Kasami	$2^{2i} - 2^i + 1$	$\gcd(i, n)=1$	$i+1$	[4], [5]
Welch	$2^t + 3$	$n = 2t + 1$	3	[6]
Niho	$2^t + 2^{\frac{t}{2}} - 1$, t even $2^t + 2^{\frac{3t+1}{2}} - 1$, t odd	$n = 2t + 1$	$\frac{t+2}{2}$ $t+1$	[7]
Inverse	$2^{2t} - 1$	$n = 2t + 1$	$n - 1$	[8], [3]
Dobbertin	$2^{4i} + 2^{3i} + 2^{2i} + 2^i - 1$	$n = 5i$	$i + 3$	[9]

Table II
KNOWN CLASSES OF QUADRATIC APN POLYNOMIAL OVER \mathbb{F}_{2^n} CCZ-INEQUIVALENT TO POWER FUNCTIONS

Functions	Conditions	Proven
$x^{2^s+1} + \alpha^{2^k-1}x^{2^{ik}+2^{mk+s}}$	$n = pk, \gcd(k, 3) = \gcd(s, 3k) = 1,$ $p \in \{3, 4\}, i = sk \bmod p, m = p - i,$ $n \geq 12, \alpha$ primitive in $\mathbb{F}_{2^n}^*$	[13]
$x^{2^{2i}+2^i} + bx^{q+1} + cx^q(2^{2i}+2^i)$	$q = 2^m, n = 2m, \gcd(i, m) = 1,$ $\gcd(2^i + 1, q + 1) \neq 1, cb^q + b \neq 0,$ $c \notin \{\lambda^{(2^i+1)(q-1)}, \lambda \in \mathbb{F}_{2^n}^*\}, c^{q+1} = 1$	[14]
$x(x^{2^i} + x^q + cx^{2^iq})$ $+ x^{2^i}(c^q x^q + sx^{2^iq}) + x^{(2^i+1)q}$	$q = 2^m, n = 2m, \gcd(i, m) = 1,$ $c \in \mathbb{F}_{2^n}, s \in \mathbb{F}_{2^n} \setminus \mathbb{F}_q,$ $X^{2^i+1} + cX^{2^i} + c^qX + 1$ is irreducible over \mathbb{F}_{2^n}	[14]
$x^3 + a^{-1}Tr_n(a^3x^9)$	$a \neq 0$	[15]
$x^3 + a^{-1}Tr_n^3(a^3x^9 + a^6x^{18})$	$3 n, a \neq 0$	[1]
$x^3 + a^{-1}Tr_n^3(a^6x^{18} + a^{12}x^{36})$	$3 n, a \neq 0$	[1]
$ux^{2^s+1} + u^{2^k}x^{2^{-k}+2^{k+s}} +$ $vx^{2^{-k}+1} + wu^{2^k+1}x^{2^s+2^{k+s}}$	$n = 3k, \gcd(k, 3) = \gcd(s, 3k) = 1,$ $v, w \in \mathbb{F}_{2^k}, vw \neq 1,$ $3 (k+s)$ u primitive in $\mathbb{F}_{2^n}^*$	[16]
$\alpha x^{2^s+1} + \alpha^{2^k}x^{2^{k+s}+2^k} +$ $\beta x^{2^k+1} + \sum_{i=1}^{k-1} \gamma_i x^{2^{k+i}+2^i}$	$n = 2k, \gcd(s, k) = 1, s, k$ odd, $\beta \notin \mathbb{F}_{2^k}, \gamma_i \in \mathbb{F}_{2^k},$ α not a cube	[17], [16]

is APN over \mathbb{F}_{2^n} .

The statement just mentioned gives new examples of APN functions in even dimensions. The following infinite families of function are proved to be APN also in odd dimensions:

- 1) $x^3 + a^{-1}Tr(a^3x^9)$, with $a \in \mathbb{F}_{2^n}^*$ and any positive n ;
- 2) $x^3 + a^{-1}Tr^3(a^6x^{18} + a^{12}x^{36})$, with $a \in \mathbb{F}_{2^n}^*$ and n divisible by 3;
- 3) $x^3 + a^{-1}Tr^3(a^3x^9 + a^6x^{18})$, with $a \in \mathbb{F}_{2^n}^*$ and n divisible by 3.

In [1] some conditions for constructing permutations, and consequentially for constructing APN functions, are given.

- For a general positive n and a linear function L over \mathbb{F}_{2^n} if for every $u \in \mathbb{F}_{2^n}$ such that $L(u) \neq 0$, the condition

$$Tr_n\left(\frac{u}{(L(u))^3}\right) = \begin{cases} 0 & \text{if } n \text{ is odd} \\ 1 & \text{if } n \text{ is even} \end{cases}$$

is satisfied, then the function $x + L(x^3)$ is a permutation.

- For n even integer and L linear function over \mathbb{F}_{2^n} the function $x + L(x^3)$ is a permutation of \mathbb{F}_{2^n} if and only if for every $b \in \mathbb{F}_{2^n}^*$ such that $L^*(b) \neq 0$ there exists an element $\gamma \in \mathbb{F}_{2^n}$ such that $L^*(b) = \gamma^3$ and $Tr_n^2(\gamma^{-1}b) \neq 0$, where L^* denotes the adjoint linear mapping of L .
- For n odd integer and L linear function over \mathbb{F}_{2^n} the function $x + L(x^3)$ is a permutation of \mathbb{F}_{2^n} if and only if for every $b \in \mathbb{F}_{2^n}$ either $L^*(b) = 0$ or $Tr_n(\gamma^{-1}b) = 0$, where $L^*(b) = \gamma^3$ and L^* denotes the adjoint linear mapping of L .

The above mentioned function $x^9 + Tr(x^3)$, for $n = 8$, is a clear example of the fact that there are other possible

conditions for function of the form (1) to be APN. Therefore with this work we try to find new conditions and new relations for the APN property.

II. APN CONDITIONS

A. Necessary and sufficient conditions

Let $F(x) = L_1(x) + L_2(x^3)$, with L_1 and L_2 as in (2), be a function defined over \mathbb{F}_{2^n} for a positive integer n and $F'(x) = F(x^3) = L_1(x^3) + L_2(x^9)$.

Just analysing the APN property for a quadratic function we can state the following lemma.

Lemma 1. For any positive integer n and any linear functions L_1 and L_2 of \mathbb{F}_{2^n} , a function F' defined by (1) is APN if and only if for every $a \in \mathbb{F}_{2^n}^*$ one of the following conditions is satisfied:

- 1) if $x \neq 0, 1$

$$L_1(a^3(x^2 + x)) + L_2(a^9(x^8 + x)) \neq 0; \quad (4)$$

- 2) if $y \neq 0$ and $Tr(y) = 0$

$$L_1(a^3y) + L_2(a^9(y^4 + y^2 + y)) \neq 0. \quad (5)$$

Proof. Since F' is a quadratic function satisfying $F'(0) = 0$, APN condition can be reformulated as the following: for any $a \in \mathbb{F}_{2^n}^*$

$$F'(ax + a) + F'(ax) + F'(a) = 0 \text{ if and only if } x \in \{0, 1\}.$$

The equation above is equivalent to $L_1(a^3(x^2 + x)) + L_2(a^9(x^8 + x)) = 0$, therefore we have that

$$L_1(a^3(x^2 + x)) + L_2(a^9(x^8 + x)) \neq 0 \text{ if and only if } x \neq 0, 1.$$

Lets denote now $y = x^2 + x$. Since $x \neq 0, 1$ we have that $y \neq 0$ and $\text{Tr}(y) = 0$. The second condition follows easily. \square

Proposition 1. Let F' be APN and, referring to (2), construct the linear function $L_3(x) = \sum_{i=0}^{n-1} d_i x^{2^i}$ with coefficients

$$d_0 = b_0 + b_{n-1} + c_0 + c_{n-3}$$

$$d_1 = b_1 + b_0 + c_1 + c_{n-2}$$

$$d_2 = b_2 + b_1 + c_2 + c_{n-1}$$

$$d_i = b_i + b_{i-1} + c_i + c_{i-3}, \text{ for } 3 \leq i \leq n-1.$$

Then L_3 is a 2-to-1 map satisfying $L_3(x) = 0$ if and only if $x = 0, 1$.

Proof. Using equation (4) with $a = 1$, consider the following map: $L_1(x^2 + x) + L_2(x^8 + x)$. Analysing the two linear functions we have: $L_1(x^2 + x) = (b_0 + b_{n-1})x + \sum_{i=1}^{n-1} (b_i + b_{i-1})x^{2^i}$, $L_2(x^8 + x) = (c_0 + c_{n-3})x + (c_1 + c_{n-2})x^2 + (c_2 + c_{n-1})x^{2^2} + \sum_{i=3}^{n-1} (c_i + c_{i-3})x^{2^i}$. Therefore $L_1(x^2 + x) + L_2(x^8 + x)$ corresponds to the linear function $L_3(x)$ described above. From Lemma 1 we have that $L_3(x) = 0$ if and only if $x = 0, 1$. \square

The following lemma gives a quite fast way to verify if a function F' can be APN, since you have to evaluate it over a third of the elements of the space.

Lemma 2. For n even assume F' is APN. Let $\alpha \in \mathbb{F}_{2^n}^*$ be a primitive element and $k = \frac{2^n-1}{3}$. Then $F'(a) \neq 0$ for any $a \neq 0$ or equivalently $F(\alpha^{3j}) = F'(\alpha^j) \neq 0$ for $0 \leq j \leq k-1$.

Proof. For n even we have $\text{Tr}(1) = 0$. Therefore using equation (5) with $y = 1$ we get for any $a \neq 0$

$$L_1(a^3) + L_2(a^9) = F(a^3) = F'(a) \neq 0.$$

For $a \neq 0$ we have that $a = \alpha^j$ with $0 \leq j \leq 2^n - 2$. Since we consider just cubic power of a , we can restrict the possibilities to $0 \leq j \leq k-1$. This concludes the proof. \square

Remark 1. If we consider $j = 0$ in Lemma 2 then

$$L_1(1) + L_2(1) = \sum_{i=0}^{n-1} b_i + \sum_{i=0}^{n-1} c_i = \sum_{i=0}^{n-1} (b_i + c_i) \neq 0.$$

Moreover, if we just consider linear functions defined over \mathbb{F}_2 (i.e. $b_i, c_i \in \mathbb{F}_2$) then a fast way to check if F' is not APN is by verifying that L_1 and L_2 have the same parity number of monomials.

Lemma 3. Let n be an even number multiple of 3 and F' be APN. Then for any $a \neq 0$ $L_1(a^3\beta) \neq 0$, with $\beta \in \mathbb{F}_{2^3}^*$ such that $\text{Tr}_3(\beta) = 0$.

Proof. Consider such an element β and call m the integer $\frac{n}{3}$. We have that $\text{Tr}_n(\beta)$ is equal to $\sum_{j=1}^m \sum_{i=0}^2 \beta^{2^i} = \sum_{j=1}^m \text{Tr}_3(\beta) = 0$. Therefore we can apply (5) with $y = \beta$ and obtain

$$L_1(a^3\beta) + L_2(a^9(\beta^4 + \beta^2 + \beta)) = L_1(a^3\beta) \neq 0 \quad \forall a \neq 0.$$

Lemma 4. Consider a function F' from \mathbb{F}_{2^n} to itself defined as in (1). F' is APN if and only if it satisfies the following condition:

for every $a, y \neq 0$ with $\text{Tr}(y)=0$ if an element $t \in \mathbb{F}_{2^n}$ satisfies $\text{Tr}(t)=0$ and

$$L_1(a^3y) = L_2(a^9y^3t)$$

then $L_2(a^9(y^4 + ty^3 + y^2 + y)) \neq 0$.

Proof. By Lemma 1 we have that APN property for F' is equivalent to

for any $a, y \in \mathbb{F}_{2^n}^*$, $\text{Tr}(y) = 0$ $L_1(a^3y) + L_2(a^9(y^4 + y^2 + y)) \neq 0$.

Assume that there exists an element t that satisfies the conditions in the statement. Let us re-write the formula above

$$\begin{aligned} 0 &\neq L_1(a^3y) + L_2(a^9(y^4 + y^2 + y)) = \\ &L_1(a^3y) + L_2(a^9y^3t) + L_2(a^9(y^4 + ty^3 + y^2 + y)) = \\ &L_2(a^9(y^4 + ty^3 + y^2 + y)). \end{aligned}$$

Therefore the APN condition is equivalent to

$$L_2(a^9(y^4 + ty^3 + y^2 + y)) \neq 0.$$

On the other hand assume that for any t of null trace we have $L_1(a^3y) \neq L_2(a^9y^3t)$. Therefore

$$L_1(a^3y) \notin \Omega = \{L_2(a^9y^3t) : \text{Tr}(t) = 0\}.$$

Let us consider the second term of the formula,

$$L_2(a^9(y^4 + y^2 + y)) = L_2(a^9y^3(y + 1/y + 1/y^2)).$$

Since $\text{Tr}(y + 1/y + 1/y^2) = 0$, the term belongs to the set Ω . Therefore the relation is again respected. \square

Corollary 1. For general $a \neq 0$ and $y \neq 0$ with $\text{Tr}(y)=0$, if the equation

$$L_1(a^3y) = L_2(a^9y^3t)$$

is satisfied only for t with $\text{Tr}(t)=1$, then the function $F'(x) = F(x^3) = L_1(x^3) + L_2(x^9)$ is APN.

Proof. In this case the hypothesis of the previous lemma is always satisfied, since there is no element t such that $L_1(a^3y) = L_2(a^9y^3t)$ and $\text{Tr}(t) = 0$. Therefore the function F' is APN. \square

B. On APN functions of the form $x^9 + L(x^3)$

From [15] we know that in \mathbb{F}_{2^8} the function $F'(x) = x^9 + \text{Tr}(x^3)$ is APN.

Lemma 5. If $3|n$ then the function $x^9 + \text{Tr}(x^3)$ is not APN over \mathbb{F}_{2^n} .

Proof. From Lemma 1 we have that $x^9 + \text{Tr}(x^3)$ is APN if and only if for any $a \neq 0$ and any $x \neq 0, 1$

$$\text{Tr}(a^3(x^2 + x)) + a^9(x^8 + x) \neq 0.$$

If we now consider n multiple of 3, $x \in \mathbb{F}_{2^3} \setminus \mathbb{F}_2$ and $a = 1$ we obtain

$$\text{Tr}(a^3(x^2 + x)) + a^9(x^8 + x) = 0.$$

□

Using Lemma 4 it was possible to implement, using the software MAGMA, a fast algorithm that checks if $x^9 + \text{Tr}(x^3)$ is APN over \mathbb{F}_{2^n} . Running the code for n up to 200 the only APN functions are for dimensions 4, 5 and 8.

Let us consider now a more general form for F' , $G(x) = x^9 + L(x^3)$ with L linear function in $\mathbb{F}_{2^n}[x]$.

With some computational work, done with MAGMA, we tried to find more APN functions of this form in other dimensions. In Table III we summarize the results we obtained. With α we indicate a primitive element of $\mathbb{F}_{2^n}^*$. We searched for APN functions in \mathbb{F}_{2^n} , up to $n = 10$, of the form $x^9 + L(x^3)$. We studied their CCZ-equivalence relation and obtained the representatives for each dimension. Obviously for every n not multiple of 3, the Gold function x^9 (corresponding to the case $L(x) = 0$) is APN.

Table III
APN FUNCTIONS OF THE FORM $x^9 + L(x^3)$ OVER \mathbb{F}_{2^n}

n	CCZ-eq	Representatives
4	1	$L(x) = 0$
5	2	$L(x) = 0, L(x) = \text{Tr}(x)$
6	2	$L(x) = \alpha^{44}x + \alpha x^2,$ $L(x) = \alpha^{23}x + x^{2^2}$
7	1	$L(x) = 0$
8	6	$L(x) = 0, L(x) = x^2 + x^{2^4},$ $L(x) = x^{2^3} + x^{2^7}, L(x) = \text{Tr}(x),$ $L(x) = x^{2^2} + \alpha^{85}x^{2^3} + x^{2^4},$ $L(x) = \alpha^{60}x + \alpha^{200}x^2 + \alpha^{242}x^4 + \alpha^{190}x^8 + \alpha x^{16}$
9	0	-
10	2	$L(x) = 0,$ $L(x) = \alpha^{1021}x + \alpha^{1022}x^2 + \alpha x^{2^2}$

For greater dimensions we just checked the possible APN function of the form $x^9 + L(x^3)$ with $L \in \mathbb{F}_2[x]$, up to CCZ-equivalence.

- for $n = 11$ there are no APN except $F(x) = x^9$;
- for $n = 12$ there are no APN;
- for $n = 13$ there are no APN except $F(x) = x^9$;
- for $n = 14$ there are no APN except $F(x) = x^9$;
- for $n = 15$ there are no APN;
- for $n = 16$ there are no APN except $F(x) = x^9$.

For $n = 4$ the function $x^9 + \text{Tr}(x^3)$ is CCZ-equivalent to the Gold function x^9 .

For $n = 6$ the found APN functions are not CCZ-equivalent to functions $x^9 + L(x^3)$ defined over \mathbb{F}_2 . Moreover we get:

- for $L(x) = \alpha^{44}x + \alpha x^2$ the function $x^9 + L(x^3)$ is CCZ-equivalent to $x^3 + \alpha^{-1}\text{Tr}_n(\alpha^3 x^9)$;

- for $L(x) = \alpha^{23}x + x^{2^2}$ the function $x^9 + L(x^3)$ is CCZ-equivalent to $x^3 = x^3 + \text{Tr}_n(x^9)$.

Both of these functions belong to the class of APN functions studied in [1]

For $n = 8$ we compared the found APN mappings with the list of known APN function in dimension 8 in [18]. We get the following:

- for $L(x) = x^2 + x^{2^4}$ the function $x^9 + L(x^3)$ is CCZ-equivalent to $x^3 + \text{Tr}(x^9)$;
- for $L(x) = x^{2^3} + x^{2^7}$ the function $x^9 + L(x^3)$ is CCZ-equivalent to x^3 ;
- for $L(x) = x^{2^2} + \alpha^{85}x^{2^3} + x^{2^4}$ the function $x^9 + L(x^3)$ is not CCZ-equivalent to any function of the form $x^3 + a^{-1}\text{Tr}(a^3 x^9)$ but it is CCZ-equivalent to function $\alpha^{135}x^{144} + \alpha^{120}x^{66} + \alpha^{65}x^{18} + x^3$, no. 6 in the list of APN mapping of \mathbb{F}_{2^8} in [18];
- for $L(x) = \alpha^{60}x + \alpha^{200}x^2 + \alpha^{242}x^4 + \alpha^{190}x^8 + \alpha x^{16}$ the function $x^9 + L(x^3)$ is not CCZ-equivalent to any function of the form $x^3 + a^{-1}\text{Tr}(a^3 x^9)$ but it is CCZ-equivalent to function $\alpha^{242}x^{192} + \alpha^{100}x^{144} + \alpha^{66}x^{132} + \alpha^{230}x^{129} + \alpha^{202}x^{96} + \alpha^{156}x^{72} + \alpha^{254}x^{66} + \alpha^{18}x^{48} + \alpha^{44}x^{36} + \alpha^{95}x^{33} + \alpha^{100}x^{24} + \alpha^{245}x^{18} + \alpha^{174}x^{12} + \alpha^{175}x^9 + \alpha^{247}x^6 + \alpha^{166}x^3$, no. 9 in the list of APN mapping of \mathbb{F}_{2^8} in [18]

C. On the number of bent components

From [19] we get the following theorem.

Theorem 1. *Let F be a function from \mathbb{F}_{2^n} to \mathbb{F}_{2^n} . Then for any non-zero $a \in \mathbb{F}_{2^n}$*

$$\sum_{\lambda \in \mathbb{F}_{2^n}} \mathcal{F}^2(D_a f_\lambda) \geq 2^{2n+1}.$$

Moreover, F is APN if and only if for every non-zero $a \in \mathbb{F}_{2^n}$

$$\sum_{\lambda \in \mathbb{F}_{2^n}} \mathcal{F}^2(D_a f_\lambda) = 2^{2n+1}.$$

Lemma 6. *$F'(x) = L_1(x^3) + L_2(x^9)$ is an APN function if and only if for any $a \in \mathbb{F}_{2^n}^*$ there exists one and only one $\lambda \in \mathbb{F}_{2^n}^*$ such that $\text{Tr}(\lambda L_1(ax^2 + a^2x) + \lambda L_2(ax^8 + a^8x))$ is constantly 0.*

Proof. Since F' is a quadratic function, every component has at most algebraic degree 2 and, consequently, the Boolean function $D_a f'_\lambda$ can be either affine or constant. If $D_a f'_\lambda$ is affine then $\mathcal{F}(D_a f'_\lambda) = 0$. In the other case we have $\mathcal{F}(D_a f'_\lambda) = \pm 2^n$ and $\mathcal{F}^2(D_a f_\lambda) = 2^{2n}$. Let consider the set

$$\Delta_a = \{\lambda \in \mathbb{F}_{2^n} : D_a f'_\lambda \text{ is constant}\}, \quad (6)$$

then

$$\sum_{\lambda \in \mathbb{F}_{2^n}} \mathcal{F}^2(D_a f'_\lambda) = 2^{2n} \cdot |\Delta_a|.$$

From the previous theorem we have that F' is APN if and only if the sum is equal to 2^{2n+1} , hence if and only if $|\Delta_a| = 2$. Since f'_0 , and consequently $D_a f'_0$, is the constantly null

function, we have that 0 belongs to the set Δ_a for every $a \neq 0$. Therefore, F' is APN if and only if $|\Delta_a^*| = 1$, with

$$\Delta_a^* = \Delta_a \setminus \{0\}. \quad (7)$$

This is true for every generic quadratic APN function $F'(x)$. In our specific case we have

$$\begin{aligned} D_a f'_\lambda(x) &= \text{Tr}(\lambda[F'(x) + F'(x+a)]) = \\ &= \text{Tr}(\lambda[L_1(ax^2 + a^2x + a^3) + \\ &\quad + L_2(ax^8 + a^8x + a^9)]) = \\ &= \text{Tr}(\lambda[L_1(ax^2 + a^2x) + L_2(ax^8 + a^8x)]) + \\ &\quad + \text{Tr}(\lambda[L_1(a^3) + L_2(a^9)]). \end{aligned}$$

In order to study its constant conditions it is sufficient to study the function $g(x) = \text{Tr}(\lambda[L_1(ax^2 + a^2x) + L_2(ax^8 + a^8x)])$. Since $g(0) = 0$, we have that if g is constant then it is the constant zero function and this concludes the proof. \square

Remark 2. Equivalently, we can study the conditions for $\text{Tr}(\lambda L_1(a^3[x^2 + x]) + \lambda L_2(a^9[x^8 + x]))$ to be the constant null function. Due to the property of the Trace function we can study the conditions for $\lambda L_1(a^3[x^2 + x]) + \lambda L_2(a^9[x^8 + x])$ to be equal to $\eta + \eta^2$, with $\eta = \eta(a, \lambda, x)$.

Recalling the notation used in the proof we defined: Δ_a as in (6) and Δ_a^* as in (7);

$$V_\lambda = \{a \in \mathbb{F}_{2^n} : D_a f'_\lambda \text{ is constant}\}; \quad (8)$$

$$V_\lambda^* = V_\lambda \setminus \{0\}. \quad (9)$$

From Proposition 1 in [20] we get that the dimension of the kernel of f_λ and n have the same parity, where the kernel of a quadratic form f is the subspace of \mathbb{F}_{2^n} $\{u \in \mathbb{F}_{2^n} : f(u+v) + f(u) + f(v) = 0 \text{ for any } v \in \mathbb{F}_{2^n}\}$. From Lemma 1 in [20] we get that, since f_λ is a quadratic Boolean function, its kernel corresponds to the subspace V_λ . Therefore we have $\dim_{\mathbb{F}_2}(V_\lambda) \equiv n \pmod{2}$.

Moreover let's consider the set

$$\Gamma_i = \{\lambda \neq 0 : \dim(V_\lambda) = i\}.$$

If Γ_i not empty then i has the same parity as n . It can be easily proved by considering a not null element λ in the set, i.e. such that $\dim V_\lambda = i$. Since the dimension of V_λ has the same parity as n , the same can be state on i .

The set Γ_0 correspond to the set of all bent components.

Corollary 2. *From Lemma 6 it is straightforward to prove that APN property for a quadratic function is equivalent to the following statement: for any $\lambda_1 \neq \lambda_2 \in \mathbb{F}_{2^n}^*$,*

$$V_{\lambda_1} \cap V_{\lambda_2} = \emptyset \quad \text{and} \quad \sum_{\lambda \neq 0} |V_\lambda^*| = 2^n - 1.$$

1) Computational Results: Using the software MAGMA we tried to verify for functions F' of form (1) defined over small dimensions the relation between the APN property and the number of bent components. From the results obtained taking random linear functions L_1, L_2 and constructing F' for $n \in \{4, 6, 8\}$ the relation seems the following one:

Conjecture 1. *For an even n , a function F' of the form (1) is APN if and only if it has exactly $\frac{2}{3}(2^n - 1)$ bent components.*

We know that this is not true for general quadratic functions. Indeed consider the quadratic APN function presented by Dillon in 2006 [21]

$$F(x) = x^3 + u^{11}x^5 + u^{13}x^9 + x^{17} + u^{11}x^{33} + x^{48};$$

defined over \mathbb{F}_{2^6} where u is a primitive element, root of the polynomial $x^6 + x^4 + x^3 + x + 1$. This function has 46 bent components and $46 > \frac{2}{3}(2^6 - 1) = 42$.

III. CONCLUSION

In this work we continued the study of quadratic functions of the form $L_1(x^3) + L_2(x^9)$ and related APN conditions. New necessary and sufficient conditions are presented in this paper. Such conditions allow us to compute a faster algorithm that checks the existence of other APN functions of such form. New results are given considering functions of the form $x^9 + L(x^3)$. Up to CCZ-equivalence new APN functions are found in different low dimensions.

REFERENCES

- [1] L. Budaghyan, C. Carlet, and G. Leander, "On a construction of quadratic APN functions", *Proceedings of IEEE Information Theory workshop ITW'09*, Oct. 2009, pp. 374-378.
- [2] R. Gold, "Maximal recursive sequences with 3-valued recursive cross-correlation functions", *IEEE Trans. Inform. Theory*, 14, 1968, pp. 154-156.
- [3] K. Nyberg, "Differentially uniform mappings for cryptography", *Advances in Cryptography, EUROCRYPT'93*, Lecture Notes in Computer Science 765, 1994, pp. 55-64.
- [4] H. Janwa, and R. Wilson, "Hyperplane sections of Fermat varieties in P^3 in char. 2 and some applications to cycle codes", *Proceedings of AAECC-10, LNCS*, vol. 673, Berlin, Springer-Verlag, 1993, pp. 180-194.
- [5] T. Kasami, "The weight enumerators for several classes of subcodes of the second order binary Reed-Muller codes", *Inform. and Control*, 18, 1971, pp. 369-394.
- [6] H. Dobbertin, "Almost perfect nonlinear power functions over $GF(2^n)$: the Welch case", *IEEE Trans. Inform. Theory*, 45, 1999, pp. 1271-1275.
- [7] H. Dobbertin, "Almost perfect nonlinear power functions over $GF(2^n)$: the Niho case", *Inform. and Comput.*, 151, 1999, pp. 57-72.
- [8] T. Beth, and C. Ding, "On almost perfect nonlinear permutations", *Advances in Cryptology-EUROCRYPT'93*, Lecture Notes in Computer Science, 765, Springer-Verlag, New York, 1993, pp. 65-76.
- [9] H. Dobbertin, "Almost perfect nonlinear power functions over $GF(2^n)$: a new case for n divisible by 5", *Proceedings of Finite Fields and Applications FQ5*, 2000, pp. 113-121.
- [10] L. Budaghyan, C. Carlet, and G. Leander, "On inequivalence between known power APN functions", *Proceedings of the International Workshop on Boolean Functions: Cryptography and Applications, BFCA 2008*, Copenhagen, Denmark, May 2008.
- [11] L. Budaghyan, C. Carlet, and A. Pott, "New Classes of Almost Bent and Almost Perfect Nonlinear Functions", *IEEE Trans. Inform. Theory*, vol.52, no. 3, Mar. 2006, pp. 1141-1152.
- [12] Y. Edel, G. Kyureghyan, and A. Pott, "A new APN function which is not equivalent to a power mapping", *IEEE Trans. Inform. Theory*, vol. 52, no. 2, Feb. 2006, pp. 744-747.
- [13] L. Budaghyan, C. Carlet, and G. Leander, "Two classes of quadratic APN binomials inequivalent to power functions", *IEEE Trans. Inform. Theory*, 54(9), 2008, pp. 4218-4229.
- [14] L. Budaghyan, and C. Carlet, "Classes of Quadratic APN Trinomials and Hexanomials and Related Structures", *IEEE Trans. Inform. Theory*, vol. 54, no. 5, May 2008, pp. 2354-2357.
- [15] L. Budaghyan, C. Carlet, and G. Leander, "Constructing new APN functions from known ones", *Finite Fields and Their Applications*, vol.15, issue 2, Apr. 2009, pp. 150-159.
- [16] C. Bracken, E. Byrne, N. Markin, and G. McGuire, "New families of quadratic almost perfect nonlinear trinomials and multinomials", *Finite Fields and Their Applications*, 14(3), 2008, pp. 703-714.

- [17] C. Bracken, E. Byrne, N. Markin, and G. McGuire, "A Few More Quadratic APN Functions", *Cryptography and Communications*, 3(1), 2011, pp. 43-53.
- [18] Y. Edel, and A. Pott, "A new almost perfect nonlinear function which is not quadratic", *IACR Cryptology ePrint Archive 2008*, 2008, pp. 313.
- [19] T.P. Berger, A. Canteaut, P. Charpin, and Y. Lang-Chapuy, "On Almost Perfect Nonlinear Functions Over \mathbb{F}_2^n ", *IEEE Trans. Inform. Theory*, Vol. 52, N. 9, Sep. 2006, pp. 4160-4170.
- [20] A. Canteaut, P. Charpin, and G. M. Kyureghyan, "A new class of monomial bent functions", *Finite Fields and Their Applications*, vol.14, issue 1, Jan. 2008, pp. 221-241.
- [21] J. F. Dillon, "APN Polynomials and Related Codes", *Polynomials over Finite Fields and Applications*, Banff International Research Station, Nov. 2006.